به نام خدا

دانشکده مهندسی کامپیوتر

پروژه پیاده سازی اول

پیاده سازی پیام رسان ساده

درس مبانی امنیت اطلاعات

استاد: دکتر نستوه طاهری جوان

تیم تدریسیاری:

رضا توسلی

سید سجاد پیشوائیان

اردیبهشت 1399

در این پروژه قصد داریم یک پیام رسان ساده را پیاده سازی نماییم که بوسیله یک تونل امن تبادل پیام و فایل انجام می‌شود. این تونل امن از دو بخش server و client تشکیل شده است که پس از پیاده سازی تونل ها، کلاینت ها می توانند تبادل متن(چت) داشته باشند یا فایل به یکدیگر انتقال دهند. این کار میتواند با command line یا با استفاده از رابط گرافیکی (GUI) صورت گیرد.

(نحوه پیاده سازی این قسمت به اختیار شماست(GUI یا command line). پیاده سازی با GUI نمره امتیازی دارد.)

به عنوان مثال در command line، اگر کاربر1 بخواهد با کاربر2 چت کند، دستور Client1 message client2را وارد میکند و پس از آن کاربر 1 پیام خود را برای کاربر2 ارسال میکند. همچنین اگر کاربر 1 بخواهد برای کاربر 2 فایلی ارسال کند، دستورClient1 file client2 وارد می کند و پس از آن کاربر1 آدرس فایل ارسالی را وارد می کند و این فایل برای کاربر 2 ارسال میشود.(client1 ارسال کننده و client2 دریافت کننده است).

(لازم نیست حتما به فرمت بالا باشد. میتوانید به هر صورت دیگر پیاده سازی کنید.)

برای امن نمودن اتصال از دو روش رمز نگاری متقارن و غیر متقارن استفاده می کنیم که توضیح آن در ادامه آمده است.

رمزنگاری متقارن:
در این قسمت یک کلید مشترک (کلید فیزیکی) به صورت رمزشده روی سرور و کلاینت وجود دارد. کلید فیزیکی دارای مدت زمان انقضا برابر با مدت زمان برقراری اتصال کلاینت به سرور می باشد. کلید جلسه(session key) نیز توسط یکی از طرفین ایجاد شده،با کلید فیزیکی رمز میشود و برای طرف دیگر ارسال میشود. این کلید نیز دارای یک برچسب زمانی(time stamp) می باشد که قابل تنظیم است و پس از انقضای آن باید کلید جلسه جدید تولید شود و فرایند بالا تکرار شود؛ مثلا هر 10 ثانیه یک کلید جلسه جدید تولید شود و قبلی منقضی شود.
دیتا(متن و فایل) باید در مبدا با استفاده از کلید جلسه رمز نگاری و مقصد رمز گشایی شود. برای راحتی کار میتوان از مد کاری CTR استفاده کرد که فقط رمز نگاری پیاده شود.

رمزنگاری غیر متقارن:

- در این قسمت برای هر ارتباط client-server، کلید عمومی و خصوصی برای هر یک از طرفین تعیین نموده و با استفاده از آن کلید جلسه را ایجاد، رمزنگاری و مبادله کنید.

- برای هر ارتباط client-server، باید جدولی برای نگهداری کلید های عمومی و خصوصی طرفین به شکل زیر ایجاد شود:

Client-side:

Client-id(name)	Client private key	Server-id(name)	Server public key

Server-side:

Server-id(name)	Server private key	Client-id(name)	Client public key

این جدول همچنین مشخص میکند طرفین باید از چه نوع کلید هایی استفاده کنند

- برای ارتباط امن، کلید جلسه را با استفاده از رمز نگاری نا متقارن مبادله کنید و سپس انواع دیتا(متن و فایل) را با استفاده از کلید جلسه مبادله کنید.(در مبدا رمزنگاری و در مقصد رمز گشایی کنید)
- هر کلید یک مدت زمان انقضای قابل تغییر دارد که پس از تمام شدن آن کلید جدید ایجاد و مبادله شود.

نکات پیاده سازی:

- برای پیاده سازی احراز اصالت پیام، بدین صورت عمل می کنیم که قبل از فرایند رمز نگاری، با استفاده از تابع درهم سازی یک MAC برای دیتا ایجاد کرده، آن را رمزنگاری کرده و می فرستیم. در مقصد رمز گشایی کرده و MAC آن را چک میکنیم. اگر نادرست بود آن را دور میریزیم و یک پیام خطا به مبدا میفرستیم. در صورتی که یکی از packet ها اشتباه ارسال شده باشد، کل دیتا را مجددا ارسال کند.(امتیازی: به جای ارسال کل دیتا، از همان packet خراب شروع به ارسال کند)
- در تمامی حالات در حد امکان خصوصیات یک محیط امن حفظ شود، مگر در حالتی که امکانپذیر نیست، برای مثال در حالتی که دو کلاینت به صورت مستقیم و بدون استفاده از سرور به یکدیگر متصل شده اند، برقراری احراز هویت امکان پذیر نیست.
- کلاینت ها تعداد محدودی کلید را می توانند دربر داشته باشند .
- استفاده از توابع کتابخانه ای حداکثر در حد انجام درهم سازی و یا رمزگذاری ممکن است و از پروتکلهای موجود نباید استفاده شود .
- انجام رمزنگاری با کلیدعمومی نیاز پردازشی بالایی دارد، در حد امکان باید آن را محدود نمود .
- سعی نمایید در حد امکان تمامی جنبه های امنیتی را در نظر بگیرید، برای مثال در صورتی که امنیت سرور و یا یک کلاینت مختل شود تا چه حد امنیت کل پیامرسان مختل می شود.
- توجه کنید که از Secure Socket های آماده نمی توانید استفاده کنید و باید یک ارتباط TCP برقرار کرده و امکانات امنیتی آن را با استفاده از موارد ذکر شده پیاده سازی کنید.

- توجه کنید که برای ارسال داده ها، بصورت Byte Stream عمل کنید تا اینکه بتوان انواع فایل ها را هم رمزنگاری کرد.
- برای تست برنامه، باید روی سیستمهای جداگانه صورت گیرد و یا اینکه از Virtual Machine استفاده شود.
- میتوانید از انواع رمز نگاری های متقارن و نامتقارن گفته شده در کلاس استفاده نمایید.

نکات دیگر

- پروژه را باید هر نفر به تنهایی پیاده سازی کند و تحویل حضوری دارد که زمان آن متعاقبا اعلام خواهد شد.
- زبان پیاده سازی پروژه آزاد است.
- کدها بررسی و در صورت وجود تطابق تقلب گرفته می شود و برای طرفین نمره **صفر** منظور میگردد.
- **تنها راه تحویل تمرین ها، آپلود آنها در مودل است. به دلیل باگ موجود در سایت درس حتما بعد از آپلود کردن یکبار فایل آپلود شده را دانلود کنید تا به درست آپلود شدن آن یقین پیدا کنید.**
- مهلت ارائه و آپلود پروژه در مودل مشخص شده است (با مقیاس ثانیه). لطفا بر اساس آن زمانبندی کنید. پروژه به هیچ وجه پس از مهلت مشخص شده تحویل گرفته نمی شود.
- پروژه را با فرمت Project1_stdName_stdNum.zip آپلود کنید.
- برای ارتباط با تدریس یاران از طریق ایمیل netsecfall2019@gmail.com در ارتباط باشید

(در قسمت subject ایمیل، **حتماً** ProjectNum(مثلا Project1) را بنویسید و سپس سوال خود را مطرح نمایید)